

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)The property of Yu Zhou seized  
incident to his arrest on July 29, 2019

Case No.

2:19-mj-650

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHED AFFIDAVIT IN SUPPORT OF THIS APPLICATION, AND ATTACHMENT A THERETO, ALL INCORPORATED HEREIN BY REFERENCE.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE THE ATTACHED AFFIDAVIT IN SUPPORT OF THIS APPLICATION, AND ATTACHMENT B THERETO, ALL INCORPORATED HEREIN BY REFERENCE.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 1831	Economic Espionage
18 U.S.C. 1832	Theft of Trade Secrets
18 U.S.C. 1343 & 1349	Wire Fraud and Conspiracy to Commit Wire Fraud

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

Aug. 19, 2019

City and state: Columbus, Ohio

Dustin Dobbs

Applicant's signature

Dustin Dobbs, SA FBI

Printed name and title

Elizabeth A. Preston Deavers

Judge's signature

Elizabeth A. Preston Deavers, U.S. Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION**

**In the matter of the search of:  
The property of Yu Zhou seized incident to  
his arrest on July 29, 2019**

Case No.

2:19-mj-650

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Dustin Dobbs, being first duly sworn, hereby depose and state as follows:

**I. INTRODUCTION**

1. As set forth in detail below, an investigation into the theft of trade secrets (intellectual property and proprietary research data) from Nationwide Children's Hospital (NCH), specifically by two former NCH employees, Yu ZHOU (ZHOU) and Li CHEN (CHEN), has been ongoing since January 2018. The facts herein establish probable cause to believe ZHOU and CHEN conspired with each other to steal trade secrets belonging to NCH, their former employer, in violation of Title 18 U.S.C. § 1831 (Economic Espionage), Title 18 U.S.C. § 1832 (Theft of Trade Secrets), and Title 18 U.S.C. §§ 1343 and 1349 (Wire Fraud and Conspiracy to Commit Wire Fraud).

2. Relevant here, I make this affidavit in support of applications for a search warrant for the property of ZHOU, believing evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1831, 1832, 1343, and 1349 will be found on said property. ZHOU was searched incident to his arrest on July 29, 2019, at the San Diego International Airport. His property was seized and entered into FBI evidence. The seized property to be searched, which is now located in the possession of the FBI at 425 West Nationwide Boulevard, Columbus, Ohio 43215, is described in the following paragraphs and in Attachment A.

## **II. AGENT BACKGROUND**

3. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since September 2017, and I am currently assigned to the Cincinnati Division, Columbus Resident Agency, as a member of the Counterintelligence Squad. I am responsible for investigating, among other crimes, the theft of trade secrets and economic espionage. I have received both formal and informal training in the detection and investigation of said offense. As a result of my training and experience, I am familiar with the federal laws relating to economic espionage and the theft of trade secrets. I have participated in various investigations, including those with a foreign counterintelligence nexus. As a federal agent, I am authorized to investigate violations of the laws of the United States.

4. I have personally participated in the investigation described herein. I have reviewed the relevant documents and reports of witness interviews during the course of this investigation. The statements contained in this affidavit are based on my own observations, document reviews, and reliable information provided to me by other law enforcement officials. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search the property described below, I have not included each and every fact learned during the course of this investigation. Rather, I have set forth those facts that I believe are necessary to establish probable cause for the search warrant sought. Where actions, conversations, and statements of others are related, they are related in part, except where otherwise indicated.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 1831, 1832, 1343, and 1349 have been committed by ZHOU and CHEN.

**III. APPLICABLE STATUTES AND DEFINITIONS**

6. The FBI is investigating ZHOU and CHEN for violations of 18 U.S.C. §§ 1831, 1832, 1343, and 1349, and the investigation has determined that there is probable cause to believe that violations of U.S. laws have occurred.

7. I am advised that 18 U.S.C. § 1831 provides in relevant part:

(a) In General.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, . . . .

shall, except as provided in subsection (b), be fined not more than \$5,000,000 or imprisoned not more than 15 years, or both

8. I am further advised that the term “foreign government” as used in 18 U.S.C. § 1831 is defined by 18 U.S.C. § 11 as “any government, faction, or body of insurgents within a country with which the United States is at peace, irrespective of recognition by the United States.”

9. I am further advised that the term “foreign instrumentality” as it’s used in 18 U.S.C. § 1831 is defined by 18 U.S.C. § 1839(1) as “any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.”

10. I am advised that 18 U.S.C. § 1832 provides in relevant part:

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

...

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

11. I am further advised that the term “trade secret” as it’s used in 18 U.S.C. §§ 1831 and 1832 is defined by 18 U.S.C. § 1839(3) as follows:

[T]he term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

12. I am advised that 18 U.S.C. § 1343 provides in relevant part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

13. I am further advised that 18 U.S.C. § 1349 prohibits anyone from attempting or conspiring to violate 18 U.S.C. § 1343.

#### **IV. INVESTIGATION AND PROBABLE CAUSE**

##### **A. Relevant Individuals and Entities**

14. ZHOU is a naturalized U.S. Citizen originally from China, the co-founder and CEO of GENEXOSOME TECHNOLOGIES, INC., and a former employee of NCH, which is located in Columbus, Ohio. ZHOU worked for NCH as a researcher in the lab of NCH Doctor 1. NCH Doctor 1's lab was focused on, among other topics, the research of exosomes (which are described in more detail below), and specifically with respect to intestinal issues in premature infants. ZHOU was the longest tenured lab member until he resigned in 2017. He worked in NCH Doctor 1's lab from 2007 until 2017. ZHOU is the spouse of CHEN.

15. CHEN is a naturalized U.S. Citizen originally from China and former employee of NCH. CHEN worked for NCH as a researcher in the lab of NCH Doctor 2. NCH Doctor 2's lab was focused on, among other topics, the research of exosomes with respect to liver fibrosis. CHEN resigned from NCH in 2018. CHEN worked at NCH from 2008 until 2018.

16. During ZHOU's and CHEN's tenures at NCH, both NCH Doctor 1's and NCH Doctor 2's respective labs focused on and utilized scientific developments with respect to exosomes in research. As described below, many of these developments are considered trade secret information (TSI) and are owned by NCH. An October 30, 2017, press release regarding Avalon GloboCare Corp., Beijing Jieteng Biotechnology Co. LTD., and GenExosome Technologies, Inc., which are three of the entities related to this warrant application, defines exosomes as: "tiny, subcellular, membrane-bound vesicles measuring 30-150 nm in diameter that are released by almost all cell types." The press release further noted that "exosomes can carry membraned and cellular proteins, as well as genetic materials that are representative of cell origin. Profiling various bio-molecules in exosomes may serve as useful biomarkers for a wide variety of diseases."

17. Beijing Jieteng Biotechnology Co. LTD. (BEIJING GENEXOSOME) is a Limited Liability Corporation established in Beijing, China in 2015 by ZHOU and CHEN. According to a press release from October 2017, and to corresponding Securities and Exchange Commission filings, BEIJING GENEXOSOME is engaged in the development of exosome technology to improve diagnosis and management of diseases. BEIJING GENEXOSOME produces research kits that are designed to be used by researchers for biomarker discovery and clinical diagnostic development, as well as for the advancement of targeted therapies. Currently, BEIJING GENEXOSOME's research kits and services are available for purchase, and the kits can be used to isolate exosomes or extract exosomal RNA/protein from serum/plasma, urine and saliva samples. As described below, these kits offer to produce the same results as the process developed at NCH. These research kits are advertised to increase the yield and purity of such samples, as well as to isolate exosomes with intact membranes. This is important, especially in the research



of diseases affecting premature babies, where the sample sizes are extremely small in volume. As part of its business, BEIJING GENEXOSOME is also seeking to decode proteomic and genomic alterations underlying a wide range of pathologies, thus allowing for the introduction of novel, non-invasive “liquid biopsies.” Its mission is focused toward diagnostic advancements in the fields of oncology, infectious diseases and fibrotic diseases, and discovery of disease-specific exosomes, all of which would provide disease-origin insight necessary to enable personalized clinical management.

18. ZHOU is the director and co-Chief Executive Officer (CEO) of GENEXOSOME TECHNOLOGIES, INC. (GENEXOSOME TECH). Up until approximately August 12, 2019, GENEXOSOME TECH’s website described the company as a leading biotechnology company focused on the development of exosome-based diagnostic and therapeutic products. Also, according to GENEXOSOME TECH’s previously active website, the company was co-founded in the United States by Avalon GloboCare Corp. and ZHOU, described on the website as a clinical scientist who has spent more than 10 years on exosome research and clinical utilization of exosomes products. The website further stated that their proprietary Exosome Isolation System has proven to be a cutting-edge technology that greatly enhances exosome isolation efficiency and exosome quality. As described below, NCH developed TSI relating to exome isolation and ZHOU directly contributed to the underlying research and had access to the TSI. Further, up until approximately August 12, 2019, the company’s website indicated that the company also developed proprietary exosome isolation systems, promoted implementation of exosome biotechnology in “liquid biopsy” and targeted therapies, and provided the global market with innovative exosome products for clinical diagnosis and treatment. Furthermore, GENEXOSOME TECH’s website



stated, prior to approximately August 12, 2019, that it had U.S. operations in New Jersey, in addition to overseas operations in Beijing, Shanghai and Wuhan in China.

19. BEIJING GENEXOSOME and GENEXOSOME TECH are related entities by way of Avalon GloboCare Corp. (AVALON). AVALON is a U.S. Corporation based out of Freehold, New Jersey. According to AVALON's website, the company is a premiere healthcare management provider and biotechnology developer, dedicated to integrating and managing global healthcare resources, empowering high-impact biomedical innovation and technologies, as well as to engaging in bio-venture investment. The co-founder and current CEO of AVALON is Dr. David Jin (JIN). According to the State of Nevada business records, AVALON formed GENEXOSOME TECH in July 2017. The records further indicate JIN is the co-CEO of GENEXOSOME TECH. According to information contained in a press release from October 2017, AVALON announced that its majority-owned subsidiary, GENEXOSOME TECH, acquired 100% of the outstanding capital stock of BEIJING GENEXOSOME. Concurrently, GENEXOSOME TECH entered into and closed an Asset Purchase Agreement with ZHOU, CEO of BEIJING GENEXOSOME, pursuant to which GENEXOSOME TECH acquired all assets, including intellectual property, patents and patent applications held by ZHOU pertaining to the business of researching, developing and commercializing exosome technologies.

#### **B. NCH Developed TSI Relating to Exome Isolation**

20. Researchers at NCH, including NCH Doctor 1 and NCH Doctor 2, and those who have worked in the respective labs of NCH Doctor 1 and NCH Doctor 2, conducted extensive work related to exosomes and exosome isolation. NCH devoted years of work and its own money to researching exosomes, which led to the discovery and creation of exosome-related trade secrets,

as defined in 18 U.S.C. § 1839(3). NCH's exosome-related trade secrets, which NCH considered confidential and proprietary, included but were not limited to the following:

a. **Trade Secret 1**, which consisted of a novel method of exosome isolation, particularly related to isolating exosomes from fluid samples as small as, and smaller than, approximately 20 microliters—all developed utilizing NCH's resources.

b. **Trade Secret 2**, which consisted of nonpublic exosome-related information, data, images, and analysis located in a file titled "6.30.17 Exosome in Beijing.pptx."

c. **Trade Secret 3**, which consisted of nonpublic exosome-related information, data, images, and analysis located in a file titled "ZhouTalk Beijing Exosome meeting.pdf.pptx."

d. **Trade Secret 4**, which consisted of nonpublic exosome-related information, data, images, and analysis located in a file titled "Figure-myography.pptx."

e. **Trade Secret 5**, which consisted of nonpublic exosome-related information, data, images, and analysis located in a file titled "57ae1b40b760826e85a6ca9a-ProposalPDF-201602."

21. Trade Secrets 1 through 5 are related to products and services used in and intended for use in interstate and foreign commerce.

22. NCH's discovery of Trade Secrets 1 through 5 was funded, at least in part, by federal grants. NCH's discovery of Trade Secrets 1 through 5, at least in part, played a role in NCH's receipt of federal grant funds.

23. Trade Secrets 1 through 5 derived independent economic value, actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who could obtain economic value from the disclosure or use of the information.

EPD  
OKD  
8-19-19

24. NCH took reasonable measures to keep its trade secrets, ~~including those in this~~  
~~Indictment~~, secret, including:

- a. NCH restricted physical access to research labs to key-card access by a small number of individuals.
- b. NCH required its employees to wear identification badges to limit access to restricted areas.
- c. NCH mandated that visitors to NCH facilities sign-in and wear identification badges.
- d. NCH required third parties to sign nondisclosure agreements before disclosing any confidential or trade secret information.
- e. Upon hiring, NCH's employees were required to sign a Confidentiality and Security Agreement, which restricted the use of all confidential information to the performance of employment duties related to NCH.
- f. Upon hiring, NCH's employees were required to sign acknowledgement of the employee handbook, which includes:
  - i. NCH's Research Conflict of Interest Policy, which required employees to disclose to NCH outside financial interests.
  - ii. NCH's Patents and Copyright Policy, which requires employees to disclose, among other things, patents and patent applications to NCH. The Patents and Copyright Policy prohibited publication and disclosure of inventions deriving from work at NCH without NCH authorization. The Patents and Copyright Policy further informed employees that NCH owned all intellectual property developed or invented by its employees, including, unless otherwise stated by NCH or policy, any technical discoveries, inventions, and non-academic work of employees using NCH facilities.
  - iii. NCH's Outside Activities Policy, which mandated a process for NCH to approve outside activities in order to avoid any conflicts of interest and commitment.
- g. NCH's computers displayed a Security Banner/Warning informing employees that NCH monitored computer activity, and that NCH's computer network was restricted.
- h. NCH also conducted periodic training for its employees on the handling of confidential information, scientific/business standards of conduct, the ownership of research data, and responsible research conduct, among other topics.

25. NCH also discovered and created trade secrets through its authorized use of equipment at the Ohio State University. Ohio State likewise took reasonable measures to protect those trade secrets.

**C. ZHOU leaves NCH and gets paid \$876,087 by GENEXOSOME TECH's parent company; NCH receives allegations of trade secret theft.**

26. On or about October 8, 2017, ZHOU emailed his resignation to NCH Doctor 1, effective on or about November 10, 2017, with his last physical day in the lab being on or about October 27, 2017. This email was sent to NCH Doctor 1 from ZHOU's NCH email account, Yu.Zhou@nationwidechildrens.org.

27. In the month following ZHOU's departure from NCH, multiple wire transfers were made from AVALON to ZHOU and CHEN's personal Chase bank account. The notable wire transfers are as follows:

- A. On or about 11/20/2017, AVALON transferred \$499,000 to ZHOU and CHEN's Chase account;
- B. On or about 11/21/2017, AVALON transferred \$200,000 to ZHOU and CHEN's Chase account;
- C. On or about 11/23/2017, AVALON transferred \$100,000 to ZHOU and CHEN's Chase account; and
- D. On or about 11/27/2017, AVALON transferred \$77,087 to ZHOU and CHEN's Chase account.
- E. According to Avalon's SEC filings, GenExosome agreed to pay ZHOU \$876,087 in cash, transfer 500,000 shares of common stock of Avalon to him and issue him 400 shares of common stock of GenExosome.

28. In or around November 2017, NCH received an anonymous letter regarding the potential theft of intellectual property, misconduct and conflict of interest by two NCH employees, ZHOU and CHEN. The letter described ZHOU as a research scientist in the lab of NCH Doctor 1, as well as being the CEO of GENEXOSOME TECH. The letter further described CHEN as a

research associate in NCH Doctor 2's lab. Furthermore, the letter addressed the fact that ZHOU and CHEN filed four patents in the People's Republic of China (PRC) on topics related to exosomes, miRNA, and liver diseases, all similar topics as those developed and researched in their respective NCH labs. The letter also described the selling of those four patents and all related intellectual property from BEIJING GENEXOSOME to AVALON and GENEXOSOME TECH, AVALON's U.S. subsidiary.

29. The investigation to date has revealed that NCH Doctor 1, in her research lab at NCH, has developed a method for isolating exosomes from very tiny samples and then purifying those samples for research. Based on interviews of NCH Doctor 1, this method was borne out of necessity, given the fact that she works with and conducts research on premature babies and is unable to obtain large bodily fluid samples. This information has never been presented in a public forum and has not been published. NCH Doctor 1 considers this method to be TSI, proprietary to her lab and NCH property. A review of the GENEXOSOME TECH website, which was active until on or about August 12, 2019, revealed a product for sale, called the "GET™ Exosome Isolation Kit." In a publicly available Avalon GloboCare press release, dated October 30, 2017, ZHOU discussed a proprietary exosome isolation system, where he represented that he was able to capture exosomes from a tiny volume of bodily fluid. This product is similar to the method developed by NCH Doctor 1 in NCH Doctor 1's lab at NCH and constitutes Trade Secret 1.

**D. Further investigation reveals ZHOU and CHEN stole NCH's TSI.**

30. The investigation to date has also revealed that, during their employment with NCH, ZHOU and CHEN forwarded at least 50 emails to and/or from their NCH email accounts to multiple personal external email accounts. Many of these emails contained NCH's TSI or information underlying or relating to NCH's TSI. ZHOU maintains three external accounts,

hereinafter referred to as ZHOU EMAIL #1 (his personal email account ending in “@gmail.com”), ZHOU EMAIL #2 (a China-based email account related to GenExosome Technologies ending in “@[shortened name of GenExosome Technologies].com”) and ZHOU EMAIL #3 (another China-based email account related to GenExosome Technologies, this one being: “[shortened name of GenExosome Technologies]@163.com”). CHEN maintains one external email account, which is her personal email account, hereinafter referred to as CHEN EMAIL #1. Relevant to this Affidavit, the representative examples below demonstrate that ZHOU and CHEN sent and received emails regarding NCH, NCH’s TSI and propriety information, GENEXOSOME TECH, AVALON, and matters related to exosomes. For example:

a. On or about April 27, 2017, ZHOU sent an email from ZHOU EMAIL #3 to his ZHOU EMAIL #1 with an attachment titled “GenExosome-- 2017.pdf.” This attachment contains information related to NCH’s TSI, specifically nonpublic exosome-related information, data, images, and analysis.

b. On or about August 24, 2017, CHEN used her NCH email account to send ZHOU EMAIL #3 an email with a PowerPoint presentation attached named “Figure-myography.pptx.” Based on interviews/investigation to date, this attachment is identified as a graph depicting the analysis of research data, all of which NCH did consider and still considers confidential, proprietary and TSI or related to TSI.

c. On or about August 25, 2017, CHEN sent CHEN EMAIL #1 an email with an attachment labeled “recommendation letter (Dr. David Jin).docx.” CHEN utilized her NCH email account to send this email.

d. On or about August 25, 2017, ZHOU sent CHEN EMAIL #1 an email with the subject line of “Fw: weekly update” and an attachment labeled, “Figure-myography.pptx.” ZHOU utilized his NCH email account to send this email.

e. On or about November 20, 2017, CHEN emailed ZHOU EMAIL #2 an email with a subject line of “report of XY test” and an attachment labeled “XY1 test 2017-11-20 15-40-00-ExperimentReport.pdf.” CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to send this email. Based on interviews/investigation to date, this attachment is identified as a report of test results regarding male mice in the lab of NCH Doctor 2. NCH did consider and still considers this research data to be confidential, proprietary, and TSI or related to TSI.

f. On or about November 21, 2017, CHEN emailed ZHOU EMAIL #2 an email with a subject line of “TEM” and it included four attachments labeled: “sample 1 45k-1.tif,” “sample 2 50k-1.tif,” “sample 5 50k-4.tif,” and “sample 5 50k-5.tif.” CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to forward this information. Based on interviews/investigation to date, these attachments are identified as images of exosomes. These images are part of a larger research data set that is currently ongoing at NCH, has not yet been published or made public, and was funded by NIH grants. NCH did consider and still considers this information confidential, proprietary, and TSI or related to TSI.

31. Additionally, the investigation has revealed that CHEN used NCH’s equipment and resources to conduct unauthorized exosome-related research and analysis on or about the following dates: November 22, 2016; June 21, 2017; September 15, 2017; September 26, 2017; October 27, 2017; November 20, 2017; and November 27, 2017. On the above-identified date of November



22, 2016, CHEN further utilized NCH's equipment and research to create a related video file titled "Genexosome kit isolated serum exomes."

32. Significantly, it appears that CHEN and ZHOU were aware that NCH had policies in place which prohibited their theft. On or about July 14, 2017, CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to email CHEN EMAIL #1, copying ZHOU EMAIL #1. The email attached a Word document quoting language from NCH policy concern the ownership of intellectual property. The language included the following provisions:

"As stated in the hospital policy, all technical discoveries, inventions, and non-academic work authored, developed, or invented by any person employed by Nationwide Children's Hospital, Inc. or its subsidiaries or by those using its facilities, is considered property of the hospital. An inventor is defined as any member of the medical staff of Nationwide Children's Hospital and/or [Ohio State University] faculty member using the facilities at Nationwide Children's Hospital. This definition also encompasses all employees of Nationwide Children's Hospital during their regular course of employment, those engaged in activities involving research or clinical investigation, all house staff, appointees, professional students, consultants and other personnel engaged in basic or applied research, testing activities or service programs at the institution."

"Patents and copyrights issued or acquired as a result of or in connection with administration, research, or other educational activities conducted by members of Nationwide Children's Hospital, Inc. and supported directly or indirectly by funds administered by Nationwide Children's Hospital, Inc. or The Research Institute at Nationwide Children's Hospital, regardless of the source of such funds, and all royalties or other revenues derived therefrom shall be the property of Nationwide Children's Hospital, Inc. Nationwide Children's Hospital, Inc. reserves the right to retain, assign, license, transfer, sell or otherwise dispose of, in whole or in part, any and all rights to, interests in, or income from any such discoveries, inventions or patents, except in cases of sponsored research projects where the terms of the research contract specifically require the assignment of patent or other rights to the sponsor."

33. The investigation to date has further revealed that, during their employment with NCH, ZHOU and CHEN engaged in communications and actions related to the Chinese state and indicative of state-sponsored activity, all with respect to NCH, NCH's trade secrets and propriety

information, GENEXOSOME TECH, AVALON, and matters related to exosomes. The following are representative examples:

34. On or about February 6, 2015, ZHOU sent an email from his NCH email address carbon copying CHEN's NCH email address. In the email, ZHOU explained that he had been authorized by the International Technology Transfer Network (ITTN), a professional organization located in China committed to promoting international technology transfer to China, "to organize an exosome science meeting," the goal of which was "to incorporate cutting-edge[]exosome[]technology[]to abundant biospecimen resource[s] in China."

35. On or about March 3, 2015, CHEN sent an email from her NCH address to CHEN EMAIL #1. Attached to the email was a grant application to the National Natural Science Foundation of China (NSFC) for funding for a research project related to the study of exosomes, MiR-503, and the development of chemotherapy resistance in ovarian cancer; the application listed CHEN as a project participant. The NSFC is overseen by China's State Council, which is the highest governing authority within the Chinese Communist Party. The NSFC promotes and finances scientific research.

36. On or about August 17, 2016, ZHOU and CHEN filed two patent applications in China related to, among other things, exosome-isolation kits and the isolation of exosomes from a small amount of serum. One application concerned exosomes, miRNA-33b, and the diagnosis of liver cancer; this application contained information related to NCH's proprietary and non-public exosome isolation method described above, as well as information related to exosomes derived from healthy human serum, which was similar to work performed in the lab of NCH Doctor 2.

37. On or about November 1, 2016, CHEN sent an email from CHEN EMAIL #1 to, among others, ZHOU EMAIL #3. Attached to the email were: a spreadsheet file regarding

ZHOU's performance in 2016 as an expert for a project administered by the Beijing Foreign Experts and Foreigners Employment Affairs Center; a word-processing document related to CHEN's performance in 2016 as an expert on behalf of Company 1 for a project administered by China's State Administration of Foreign Expert Affairs; and an expert registration form listing CHEN as employed by NCH.

38. On or about May 7, 2017, CHEN sent an email from CHEN EMAIL #1 to, among others, ZHOU EMAIL #1. Attached to the email was a file titled "ISEV Poster (05.07.17).ppt"; at the top of file were the words "CHARACTERIZATION OF SALIVA EXOSOMES AND EXOSOMAL MICRORNAS IN PATIENTS WITH ORAL LEUKOPLAKIA," which were flanked on one side by a graphic for the "Beijing Stomatological Hospital" and on the other side by a graphic for NCH. A sentence of text at the bottom corner of the document stated: "This work is funded by China, Beijing Municipal Administration of Hospitals Key Medical Project (ZYLX201407)."

39. On or about August 1, 2017, ZHOU received a payment from China's State Administration of Foreign Expert Affairs (SAFEA) regarding technical direction and exchange provided during the following time periods: April 16, 2017, to April 24, 2017; June 10, 2017, to June 18, 2017; and June 27, 2017, to July 4, 2017. According to its website, SAFEA is responsible for, among other things, the employment of "foreign experts to work in the Chinese mainland," "[a]dministering relevant international exchanges and cooperation," and "[u]ndertaking other matters assigned by the PRC's State Council and the PRC's Ministry of Human Resources and Social Security."

40. On or about August 1, 2017, CHEN received a payment from China's SAFEA regarding technical direction and exchange provided during the following time periods: February

16, 2017, to February 21, 2017; March 17, 2017, to March 27, 2017; and June 28, 2017, to July 4, 2017.

41. On or about August 8, 2017, CHEN sent an email from CHEN EMAIL #1 to ZHOU EMAIL #1. Attached to the email was a document evaluating ZHOU's and CHEN's participation as experts in 2017 regarding a project administered by SAFEA.

42. On or about August 14, 2017, CHEN emailed, from her NCH email account to CHEN EMAIL #1, a draft recommendation letter purporting to be written by JIN in support of CHEN's application to the Beijing Overseas Talent Plan; the letter referred to CHEN's role at NCH as a researcher, including her work researching exosomes and exosome isolation.

43. On or about August 25, 2017, CHEN sent an email from CHEN EMAIL #1 to an address ending in "@163.com." Attached to the email was a grant application to the NSFC for funding for a research project related to oral leukoplakia and exosome-related microRNA therapy; the application, which listed CHEN as a participant, contained nonpublic exosome-related information, data, images, and analysis from NCH.

#### **E. Additional Use of External Email Accounts Relevant to this Affidavit**

44. On or about April 12, 2017, Li Meng, Chief Operating Officer of AVALON sent ZHOU and CHEN an email with a subject line of "LOI Discussion – 0412" and it included an attachment labeled "Re-GenExo Consideration-0412.pdf." JIN was cc'd on this email at his AVALON email account, as well as at his personal email account. The attachment discussed compensation, titles and stock options related to the acquisition of GENEXOSOME TECH by AVALON.

45. On or about May 19, 2017, ZHOU, from ZHOU EMAIL #3 sent an email to himself at ZHOU EMAIL #1 with a subject line of "Fw: Meeting Minutes – GenExo Meeting BJ

2017Apr19.” The email included an attachment labeled “Meeting Minutes – GenExo Meeting BJ 2017Apr19.docx.” The original email was sent on or about April 19, 2017, from Billy Lyu, Deputy General Manager of AVALON, to ZHOU EMAIL #2, Li Meng, and JIN at both his AVALON email account and another account used by JIN. The attachment discusses an AVALON company meeting held in Beijing on April 19, 2017, the participants of which included ZHOU, JIN, LI and LYU. Several items were discussed to include: GENEXOSOME TECH and the acquisition by AVALON, current GENEXOSOME TECH products, clinical studies, IP and Patents, as well as an agenda for the “International Scientific Forum on Exosome Research and Application 2017 (ISFARA).” AVALON and GENEXOSOME TECH were cited as co-sponsors of the event, which was stated to be held in Beijing, China from June 30, 2017 – July 1, 2017.

46. On or about June 30, 2017, AVALON and GENEXOSOME TECH co-sponsored the “International Scientific Forum on Exosome Research and Application 2017” (ISFARA) in Beijing, China. JIN was listed as the Moderator of the event. CHEN was scheduled to give a keynote speech entitled “Fighting liver fibrosis with exosomes,” and ZHOU giving a podium presentation entitled “An emerging role of stem cell-exosomes in regenerative medicine.” Both ZHOU and CHEN were listed as representing NCH. NCH was not aware of this conference, nor did they give permission for ZHOU and/or CHEN to present data, give a speech or provide a presentation at this event.

47. On or about August 25, 2017, CHEN sent chenliandzhouyu@gmail.com an email with an attachment labeled, “recommendation letter (Dr. David Jin).docx.” CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to send this email. (This was referenced earlier in Paragraph 32i, but included again as it relates to JIN.)

48. On or about October 9, 2017, JIN forwarded ZHOU at ZHOU EMAIL #1 an email with an attachment labeled “tcmime.2771.3123.3341.bin.” The attachment contained an exosome-related market and industry analysis forecast report conducted by Allied Market Research in Portland, OR. The report was published in September 2016.

**F. There is probable cause to believe evidence of the Subject Offenses will be found in the items described in Attachment A.**

49. On July 29, 2019, ZHOU was arrested at the San Diego International Airport and searched incident to his arrest. His property was seized and entered into FBI evidence. The property, which is described more particularly in Attachment A, contained multiple Apple iPhones and electronic storage devices. According to the review of ZHOU and CHEN’s NCH IT activity and search warrant return information, their email header information showed the two communicated via multiple personal email addresses and multiple emails contained the following wording, “Sent from my iPhone.” A Grand Jury Subpoena sent to Apple, Inc. revealed ZHOU and CHEN own several iPhones and iPads.

50. As described above, ZHOU and CHEN accessed electronic files containing TSI while employed by NCH. Additionally, as also described above, ZHOU possessed electronic files which were tailored for presentations in China and he conducted business in China. On July 29, 2019, when ZHOU was apprehended pursuant to a previously issued arrest warrant, ZHOU was returning from China. As a result, there is probable cause to believe ZHOU was keeping electronic files related to NCH’s TSI or other evidence of the Subject Offenses in the cellular telephones, electronic storage devices, and other property described in Attachment A.

**G. Computers, Electronic Storage, and Forensic Analysis**

51. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises, in whatever form they are found. One

form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

52. *Probable cause:* I submit that if a computer or storage medium is found on the premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few



examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

53. Forensic evidence: As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpatng the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

54. *Necessity of seizing or copying entire computers or storage media:* In most cases, a thorough search of a premises for information that might be stored on storage media requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence

of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt to do so on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

55. *Nature of examination:* Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

#### **H. Summary**

56. The above referenced attachments include images of exosomes captured utilizing highly sophisticated, scientific equipment belonging to NCH, as well as graphs, charts and documents depicting exosomes, to include analysis of ongoing or past research, all funded by National Institutes of Health (NIH) grants, with work being conducted on NCH property and with NCH resources.

57. Images and research data similar to those sent as attachments in the above referenced emails have appeared on marketing materials for GENEXOSOME TECH products. The referenced product marketing materials were publicly available on the GENEXOSOME TECH website until approximately August 12, 2019.

58. The above identified emails and each of their accompanying attachments pertain to the same subject areas as the work being conducted by GENEXOSOME TECH, as well as the products GENEXOSOME TECH markets and sells. The information identified in several of the email attachments is proprietary and highly marketable scientific information developed and derived from NIH grant funding at NCH. The emails, as well as the above information regarding BEIJING GENEXOSOME, GENEXOSOME TECH and AVALON, and the payments to ZHOU and CHEN from AVALON, provide probable cause that ZHOU and CHEN took this proprietary information from NCH with the intention of profiting from such information in the creation and sales of related and derivative products.

59. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the property of ZHOU, described in Attachment A, will contain evidence, fruits, and instrumentalities of the Subject Offenses, 18 U.S.C. §§ 1343, 1349, 1831, and 1832.


**V. CONCLUSION**

60. The evidence stated herein establishes probable cause to believe that ZHOU and CHEN have violated U.S. law regarding Title 18 U.S.C. § 1831, Economic Espionage and Title 18 U.S.C. § 1832, Theft of Trade Secrets, and Title 18 U.S.C. §§ 1343 and 1349, Wire Fraud and Conspiracy to Commit Wire Fraud. There is further probable cause to believe that evidence, fruits, and instrumentalities of this crime will be found on the subject property, as described more particularly in Attachment A. Based on the foregoing, I request that the Court issue the proposed search warrant.

**VI. REQUEST FOR SEALING**


61. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, tamper with or destroy evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

  
\_\_\_\_\_  
Dustin Dobbs  
Special Agent  
Federal Bureau of Investigation



Subscribed and sworn to before me on August 19, 2019

  
Honorable Elizabeth A. Preston Leathers  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**  
**Property to Be Searched**

On July 29, 2019, Yu Zhou was arrested at the San Diego International Airport. Incident to his arrest, his carry-on and checked baggage were seized, inventoried and placed into FBI evidence. The previously mentioned property to be searched, which is now located in the possession of the FBI at 425 West Nationwide Boulevard, Columbus, Ohio 43215, is further described as follows:

1. Black backpack containing the following:
  - a. USB KBI Biopharma
  - b. USB – U9HGD7d
  - c. USB PNY, 32GB
  - d. Seagate Portable Drive, S/N: NA7RGC3W
  - e. Generation Think Pad X1, S/N: PF-1L5N5T
  - f. iPhone, IMEI: 358806095547830
  - g. iPhone, IMEI: 353824086037880
  - h. iPhone, IMEI: 359257066055180
  - i. Digital Currency Card, Account Number 110034856566
  - j. Bank of China, USB key and package
  - k. Various business related documents and checkbook
- l. Brown wallet containing various ID cards, credit cards and currency
  - i. The currency was counted for inventory purposes, totals were:
    1. 101 USD
    2. 1648.10 RMB

**ATTACHMENT B**  
**Items to be Seized**

All records relating to violations of 18 U.S.C. §§ 1831, 1832, 1343, or 1349, those violations involving Yu ZHOU, Li CHEN, and any officers, directors, shareholders, employees, agents, or contractors of Avalon GloboCare Corp., GenExosome Technologies Inc., Beijing Jieteng Biotechnology Co. Ltd. a/k/a Beijing GenExosome—including but not limited to David JIN, Li MENG, and Billy LYU—and occurring after January 1, 2017, including but not limited to:

- a. Records and information relating to a conspiracy to defraud and steal trade secrets from Nationwide Children's Hospital.
- b. Records and information relating to a conspiracy to steal trade secrets, with the knowledge or intent that such theft or misappropriation would benefit a foreign government, foreign instrumentality, or foreign agent.
- c. Records and information relating to the purchase or acquisition of intellectual property from ZHOU or CHEN.
- d. Records and information relating to the state of mind of any officers, directors, shareholders, employees, agents, or contractors of Avalon GloboCare Corp., GenExosome Technologies Inc., Beijing Jieteng Biotechnology Co. Ltd. a/k/a Beijing GenExosome—including but not limited to JIN, MENG, or LYU—as it relates to the crimes under investigation and as it relates to the purchase or acquisition of stock, intellectual property, or other property from ZHOU or CHEN.
- e. Records and information relating to the formation of GenExosome Technologies, Inc.
- f. Records and information relating to the acquisition of Beijing Jieteng Biotechnology Co. Ltd. a/k/a Beijing GenExosome.
- g. Records and information relating to untrue statements of material fact or failures to disclose material facts in connection with the purchase or sale of any security, including

but not limited to shares of stock in GenExosome Technologies, Inc., or the acquisition of Beijing Jieteng Biotechnology Co. Ltd. a/k/a Beijing GenExosome.

- h. Records and information relating to the Asset Purchase Agreement between GenExosome Technologies Inc. and ZHOU dated October 25, 2017.
- i. Records and information relating to the Stock Purchase Agreement between GenExosome Technologies Inc., Beijing Jieteng (GenExosome) Biotech Co. Ltd. and ZHOU dated October 25, 2017.
- j. Records and information relating to the Executive Retention Agreement between GenExosome Technologies Inc. and ZHOU dated October 25, 2017.
- k. Records and information relating to the Invention Assignment, Confidentiality, Non-Compete and Non-Solicit Agreement between GenExosome Technologies Inc. and ZHOU dated October 25, 2017.
- l. Records and information relating to the Securities Purchase Agreement between Avalon GloboCare Corp. and GenExosome Technologies Inc. dated October 25, 2017.
- m. Records and information relating to any intellectual property held or nominally held at any point by ZHOU or CHEN, including but not limited to the following four Chinese patents: patent related to patent application number CN 2016 1 0675107.5 (application of an Exosomal MicroRNA in plasma as biomarker to diagnosis liver cancer), patent related to patent application number CN 2016 1 0675110.7 (clinical application of circulating exosome carried miRNA-33b in the diagnosis of liver cancer), patent related to patent application number CN 2017 1 0330847.X (saliva exosome based methods and composition for the diagnosis, staging and prognosis of oral cancer) and patent related to patent application number CN 2017 1 0330835.7 (a novel exosome-based

therapeutics against proliferative oral diseases); and including but not limited to any representations by or on behalf of ZHOU or CHEN regarding their ownership or other property interest in any intellectual property.

- n. Records and information relating to Nationwide Children's Hospital, including but not limited to any representations by or on behalf of ZHOU or CHEN regarding the terms of their employment at Nationwide Children's Hospital.
- o. Records and information relating to the isolation of exosomes or the GET™ Exosome Isolation Kit.
- p. Records and information relating to any financial transaction or other movement of any things of value, including but not limited to cash and shares of stock, to ZHOU or CHEN, as well as any documents, including but not limited to Forms 1099 and Forms W-2, filed with any taxing authority in connection with those transactions.
- q. Records and information relating to any communications between any officer, director, shareholder, employee, agent, or contractor of Avalon GloboCare Corp., GenExosome Technologies Inc., Beijing Jieteng Biotechnology Co. Ltd. a/k/a Beijing GenExosome, and ZHOU or CHEN.
- r. Records and information relating to communications with, or receipt of funds or other things of value from, any agent, instrumentality, arm, or program of the People's Republic of China, including but not limited to the International Technology Transfer Network, National Natural Science Foundation of China, China's State Council, the Chinese Communist Party, China's State Administration of Foreign Expert Affairs, Beijing Foreign Experts and Foreigners Employment Affairs Center, and Beijing Overseas Talent Plan.

- s. Records and information relating to the purpose of any overseas travel of ZHOU or CHEN.
- t. Records and information relating to a meeting in China on or about April 19, 2017 regarding in part GenExosome Technologies' and Avalon's business dealings related to exosome isolation kits; clinical studies in China related to liver fibrosis and various types of cancer; and the International Scientific Forum on Exosome Research and Application (ISFARA), which was scheduled to occur on or about June 30, 2017.
- u. Records and information relating to ISFARA, an event in Beijing that occurred on or about June 30, 2017 through on or about July 1, 2017.
- v. Records and information relating to communications between David Jin and any person associated with the Beijing Overseas Talent Plan regarding ZHOU or CHEN.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities



described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review

